

# Konfigurieren von Dual-ISP VTI auf FTD, das von FMC verwaltet wird

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Grundlegende Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationen auf FMC](#)

[Topologiekonfiguration](#)

[Endgerätekonfiguration](#)

[IKE-Konfiguration](#)

[IPsec-Konfiguration](#)

[Routing-Konfiguration](#)

---

## Einleitung

In diesem Dokument wird die Bereitstellung einer dualen ISP-Konfiguration mithilfe von virtuellen Tunnelschnittstellen auf einem vom FMC verwalteten FTD-Gerät beschrieben.

## Voraussetzungen

### Grundlegende Anforderungen

- Ein grundlegendes Verständnis von Site-to-Site-VPNs wäre von Vorteil. Dieser Hintergrund hilft Ihnen, den VTI-Einrichtungsprozess, einschließlich der grundlegenden Konzepte und Konfigurationen, zu verstehen.
- Grundlegende Informationen zur Konfiguration und Verwaltung von VTIs auf der Cisco FirePOWER-Plattform sind von entscheidender Bedeutung. Dazu gehören Kenntnisse über die Funktionsweise von VTIs innerhalb des FTD und deren Steuerung über die FMC-Schnittstelle.

### Verwendete Komponenten

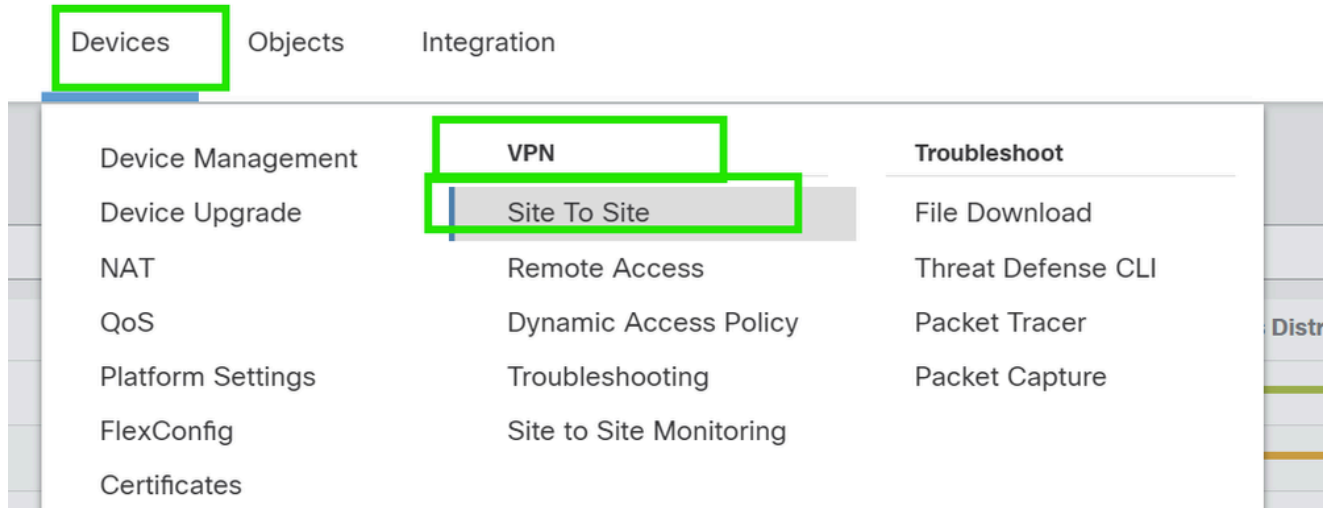
- Cisco Firepower Threat Defense (FTD) für VMware: Version 7.0.0
- FirePOWER Management Center (FMC): Version 7.2.4 (Build 169)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

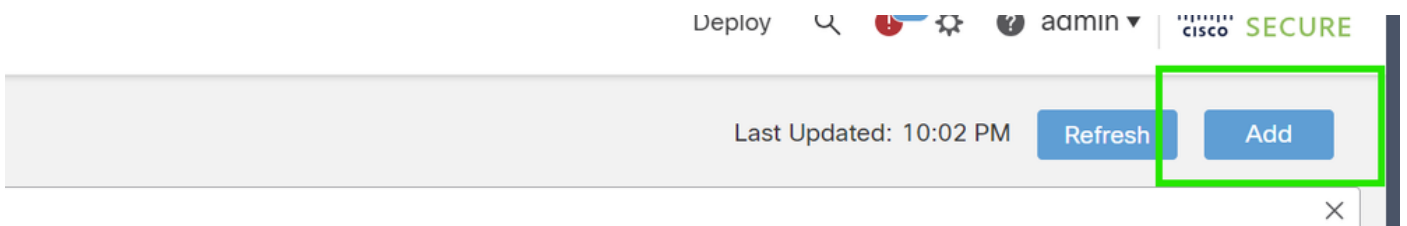
# Konfigurationen auf FMC

## Topologiekonfiguration

1. Navigieren Sie zu Geräte > VPN > Site-to-Site.



2. Klicken Sie auf Hinzufügen, um die VPN-Topologie hinzuzufügen.



3. Geben Sie einen Namen für die Topologie ein, wählen Sie VTI und Point-to-Point aus, und wählen Sie eine IKE-Version aus (in diesem Fall IKEv2).



## Endgerätekonfiguration

1. Wählen Sie das Gerät, auf dem der Tunnel konfiguriert werden soll.

Fügen Sie die Details des Remote-Peers hinzu.

Sie können entweder eine neue virtuelle Vorlagenschnittstelle hinzufügen, indem Sie auf das Symbol "+" klicken, oder Sie wählen eine Schnittstelle aus der vorhandenen Liste aus.

Endpoints IKE IPsec Advanced

**Node A**

Device:\*  
New\_FTD

Virtual Tunnel Interface:\*  
[ ] +

Tunnel Source IP is Private [Edit VTI](#)

Send Local Identity to Peers

[+ Add Backup VTI \(optional\)](#)

Connection Type:\*  
Bidirectional

**Node B**

Device:\*  
Extranet

Device Name\*:  
VTI-Peer

Endpoint IP Address\*:  
10.10.10.2

Cancel Save

Wenn Sie eine neue VTI-Schnittstelle erstellen, fügen Sie die richtigen Parameter hinzu, aktivieren Sie diese, und klicken Sie auf "OK".

HINWEIS: Dies wird zum primären VTI.

## Add Virtual Tunnel Interface



### General

Name:\*

VTI-1

Enabled

Description:

This is the primary VTI tunnel.  
This VTI goes through ISP 1.

Security Zone:

OUT

Priority:

0

(0 - 65535)

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

1

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/0 (outside1)

10.106.52.104

### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4  IPv6

192.168.10.1/30

Cancel

OK

3. Klicken Sie auf "+ ". Fügen Sie "Backup VIT" hinzu, um ein sekundäres VIT hinzuzufügen.

Device:\*

10.106.50.55 ▼

Virtual Tunnel Interface:\*

VTI-1 (IP: 192.168.10.1) ▼ +

Tunnel Source: *outside1 (IP: 10.106.52.104)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

+ Add Backup VTI (optional)

Connection Type:\*

Bidirectional ▼

Additional Configuration ⓘ

Route traffic to the VTI : [Routing Policy](#)

Permit VPN traffic : [AC Policy](#)

4. Klicken Sie auf "+", um den Parameter für den sekundären VTI hinzuzufügen (falls nicht bereits konfiguriert).

10.106.50.55 ▼

Virtual Tunnel Interface:\*

VTI-1 (IP: 192.168.10.1) ▼



*Tunnel Source: outside1 (IP: 10.106.52.104)* [Edit VTI](#)

Tunnel Source IP is Private

Send Local Identity to Peers

---

Backup VTI:

[Remove](#)

Virtual Tunnel Interface:\*

▼



Tunnel Source IP is Private

[Edit VTI](#)

Send Local Identity to Peers

---

Connection Type:\*

5. Wenn Sie eine neue VTI-Schnittstelle erstellen, fügen Sie die richtigen Parameter hinzu, aktivieren Sie sie, und klicken Sie auf "OK".

HINWEIS: Dies wird zum sekundären VTI.

## Add Virtual Tunnel Interface



### General

Name:

VTI-2

Enabled

Description:

This is the secondary VTI tunnel..  
VTI goes through ISP 2.

Security Zone:

OUT

Priority:

0

(0 - 65535)

### Virtual Tunnel Interface Details

An interface named Tunnel<ID> is configured. Tunnel Source is a physical interface where VPN tunnel terminates for the VTI.

Tunnel ID:\*

2

(0 - 10413)

Tunnel Source:\*

GigabitEthernet0/1 (outside2)

10.106.53.10

### IPsec Tunnel Details

IPsec Tunnel mode is decided by VPN traffic IP type. Configure IPv4 and IPv6 addresses accordingly.

IPsec Tunnel Mode:\*

IPv4  IPv6

192.168.20.1/30



Cancel

OK

## IKE-Konfiguration

1. Navigieren Sie zur Registerkarte IKE. Sie können eine vordefinierte Richtlinie verwenden, indem Sie auf die Bleistiftschaltfläche neben der Registerkarte "Richtlinie" klicken, um eine neue Richtlinie zu erstellen, oder eine andere verfügbare Richtlinie auswählen, die Ihren Anforderungen


entspricht.

Endpoints **IKE** IPsec Advanced

Authentication Type: Pre-shared Automatic Key

Pre-shared Key Length:\* 24 Characters (Range 1-127)



IKEv2 Settings

Policies:\* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Automatic Key


Pre-shared Key Length:\* 24 Characters (Range 1-127)

## IKEv2 Policy ?

Available IKEv2 Policy  

- AES-GCM-NULL-SHA
- AES-GCM-NULL-SHA-LAT...
- AES-SHA-SHA
- AES-SHA-SHA-LATEST
- Arko\_Test\_IKEv2
- DES-SHA-SHA

Selected IKEv2 Policy

AES-GCM-NULL-SHA-LATEST 

2. Wählen Sie den Authentifizierungstyp aus. Wenn ein vorinstallierter manueller Schlüssel verwendet wird, geben Sie den Schlüssel in den Feldern Schlüssel und Schlüssel bestätigen ein.



## IKEv2 Settings

Policies:\* AES-GCM-NULL-SHA-LATEST 

Authentication Type: Pre-shared Manual Key ▼

Key:\* .....

Confirm Key:\* .....

 Enforce hex-based pre-shared key only

Cancel

Save

## IPsec-Konfiguration

Navigieren Sie zur Registerkarte IPsec. Sie können ein vordefiniertes Angebot verwenden, indem Sie auf das Bleistiftsymbol neben der Registerkarte "Angebot" klicken, um ein neues Angebot zu erstellen, oder ein anderes verfügbares Angebot auf Basis Ihrer Anforderung auswählen.

IKEv2 Mode: Tunnel ▼

Transform Sets: IKEv1 IPsec Proposals  IKEv2 IPsec Proposals\* 

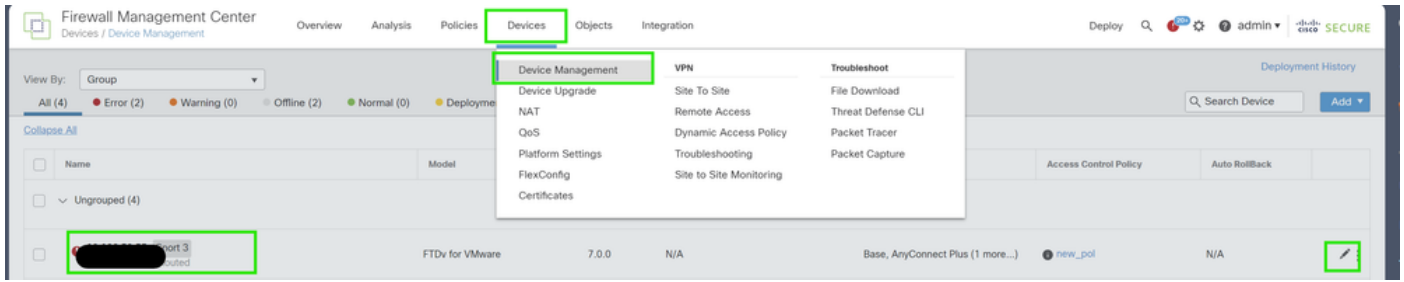
tunnel\_aes256\_sha

AES-GCM

- Enable Security Association (SA) Strength Enforcement
- Enable Reverse Route Injection
- Enable Perfect Forward Secrecy

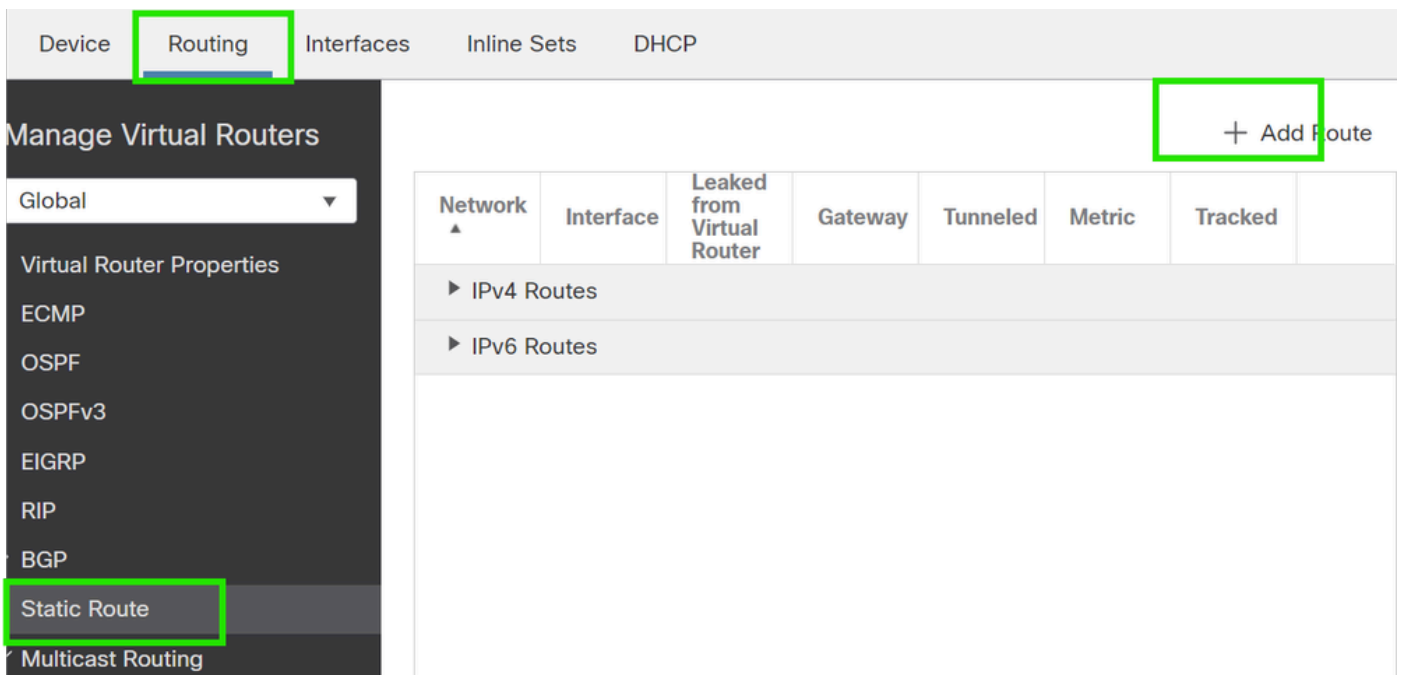
## Routing-Konfiguration

1. Gehen Sie zu Gerät > Gerätemanagement und klicken Sie auf das Bleistiftsymbol, um das Gerät (FTD) zu bearbeiten.



2. Gehen Sie zu Routing > Static Route, und klicken Sie auf die Schaltfläche "+", um eine Route zum primären und sekundären VTI hinzuzufügen.

HINWEIS: Sie können die geeignete Routing-Methode für den Datenverkehr konfigurieren, der die Tunnelschnittstelle passiert. In diesem Fall wurden statische Routen verwendet.



3. Fügen Sie zwei Routen für Ihr geschütztes Netzwerk hinzu, und legen Sie einen höheren AD-Wert (in diesem Fall 2) für die sekundäre Route fest.

Die erste Route verwendet die VTI-1-Schnittstelle, die zweite die VTI-2-Schnittstelle.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric
▶ IPv4 Routes					
protected-network	VTI-1	Global	VTI-1-Gateway	false	1
protected-network	VTI-2	Global	VTI-2-Gateway	false	2

## Überprüfung

1. Gehen Sie zu Devices > VPN > Site to Site Monitoring .

Devices

Objects

Integration

Device Management

Device Upgrade

NAT

QoS

Platform Settings

FlexConfig

Certificates

VPN

Site To Site

Remote Access

Dynamic Access Policy

Troubleshooting

Site to Site Monitoring

Troubleshoot

File Download

Threat Defense CLI

Packet Tracer

Packet Capture

2. Klicken Sie auf das Auge, um weitere Details über den Status des Tunnels zu überprüfen.



View full information

Dual-ISP-VTI

Active

2024-06-11 06:55:26

Dual-ISP-VTI

Active

2024-06-12 14:27:22

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.